หมั่นดูแลและรักษา ข้อมูล

ข้อมูลคือสิ่งมีค่า การดูแลรักษาจึงเป็นสิ่งจำเป็น คุณดูแลข้อมูลของคุณดีแค่ไหน

ลองจินตนาการความรู้สึกของคุณ เมื่อคุณได้รับรู้ว่าข้อมูลที่คุณเก็บไว้ในเครื่องคอมพิวเตอร์ของคุณได้อันตรธานหายไป คุณมีข้อมูลชุดใหม่ที่จะโหลดลงไปได้หรือไม่ หรือว่าคราวนี้งานของคุณจะต้องล่มจมหมดแล้วสิ่งต่าง ๆ เหล่านี้เกิดขึ้นได้เสมอ และมีโอกาสเกิดขึ้นได้ตลอดเวลา อาจจะเกิดจากความพลั้งเผลอ หรือเกิดจากการใช้งานผิดพลาด เกิดจากความผิดพลาดในการทำงานของฮาร์ดแวร์ เกิดจากไวรัสคอมพิวเตอร์ ฯลฯ

ในการดำเนินงานทั่วไปคุณอาจต้องลงทุนในระบบงานไปไม่ใช่น้อย มีการเก็บรักษาข้อมูลไว้ใช้งาน ข้อมูลเหล่านั้นต้องใช้เวลาและใช้กำลังแรงงานจำนวนมากเพื่อการเก็บเข้าไว้ในระบบ ดังนั้นข้อมูลในระบบจึงเป็นสิ่งที่มีค่า การดูแลรักษาข้อมูลจึงเป็นสิ่งที่จำเป็นและต้องให้ความสำคัญ

อย่ามองข้ามความปลอดภัย

การดูแลรักษาความปลอดภัยจึงเป็นหัวข้อที่มีผู้กล่าวถึงและให้ความสำคัญ ทั้งในระดับผู้ออกแบบเครื่องคอมพิวเตอร์ โปรแกรมโอเอส ยูทิลิตี้ การพัฒนาระบบงาน การปฏิบัติงานของผู้ใช้ หรือแม้แต่การให้ความปลอดภัยจากการโจรกรรมหรือเรียกค้นดูข้อมูล คัดลอกข้อมูลโดยผู้ไม่มีส่วนเกี่ยวข้อง งานด้านความปลอดภัยของข้อมูลจึงเกี่ยวกับเรื่องสำคัญต่อไปนี้

1. การป้องกันข้อมูล ซึ่งเกี่ยวข้องกับการจัดเก็บ การสำเนา การสำรอง และการให้ข้อมูลเก็บในตัวกลางโดยปลอดภัย

2. การป้องกันจากผู้อื่นมาเรียกใช้คัดลอกข้อมูล เป็นวิธีการสร้างระบบให้ผู้ที่เกี่ยวข้องกับการดูแลข้อมูลเป็นผู้ดำเนินการได้ แยกแยะระดับการใช้ การเรียกดู หรือแบ่งกลุ่มข้อมูลเพื่อการใช้งานตามหน้าที่ของบุคคลที่เกี่ยวข้อง

3. การป้องกันจากไวรัสคอมพิวเตอร์ เป็นเรื่องที่มีปัญหาและมีโอกาสจากไวรัสที่จะเข้ามามีส่วนทำให้ข้อมูลเสียหายได้

4. ป้องกันคอมพิวเตอร์ของคุณให้ปลอดภัย การป้องกันจากการโดนขโมย หรือการเสียหายโดยพลั้งเผลอ

กลยุทธ์ในการสำรองข้อมูล

การสำรองข้อมูลเป็นกิจวัตรประจำวันที่ต้องทำ สมมติว่าคุณมีระบบงานหนึ่งที่ทำด้วยคอมพิวเตอร์อยู่เป็นประจำ ในตัวระบบคอมพิวเตอร์จะประกอบด้วยโปรแกรมและข้อมูล โปรแกรมเป็นสิ่งที่เก็บอยู่ในคอมพิวเตอร์เพื่อเรียกใช้งาน โปรแกรมอาจไม่เปลี่ยนแปลงนักจนกว่าคุณจะเปลี่ยนแปลงเวอร์ชันหรือมีการเพิ่มเติมแก้ไข ข้อมูลจะมีเพิ่มขึ้นหรือเปลี่ยนแปลงแก้ไขได้ทุกวัน การดำเนินงานเกี่ยวกับข้อมูลจึงเกิดขึ้นตลอดเวลา

การสำเนาข้อมูลทำได้หลายรูปแบบ เช่น การสำเนาข้อมูลทั้งหมด ซึ่งหมายถึงการสำรองข้อมูลทั้งโปรแกรมและข้อมูล หากระบบงานมีการจัดเก็บเป็นไดเรคทอรีเรียบร้อย การสำรองข้อมูลอาจทำได้โดยใช้คำสั่ง XCOPY ในดอส หรือการเลือกสำรองข้อมูลบางส่วน การเลือกบางส่วนทำให้การทำงานเร็วขึ้น อาจมีการเลือกข้อมูลเฉพาะในส่วนที่มีการเปลี่ยนแปลง หรือเลือกเฉพาะบางแฟ้มที่มีการปรับปรุง การสำเนาบางส่วนอาจทำไว้ในโปรแกรม เช่น เมื่อเลิกงานก็เลือกเมนูที่สั่งให้สำรองข้อมูล โปรแกรมจะเลือกแฟ้มข้อมูลเฉพาะส่วนที่สำคัญเท่านั้น การกระทำการสำรองบางส่วนจึงอาจต้องเตรียมการและกระทำไว้ในโปรแกรมเพื่อให้ผู้ใช้ใช้งานได้ง่าย

การสำรองข้อมูลจึงเป็นขั้นตอนที่เพิ่มเติมจากการทำงานโดยปกติ ปัญหาจึงอยู่ที่ผู้ปฏิบัติงานมักไม่กระทำตามหรือละเลยในทางปฏิบัติ ทำให้ลดความสำคัญของการสำรอง และหากเกิดปัญหาขึ้นจะสร้างผลเสียหายที่ร้ายแรงได้

การสำรองข้อมูลส่วนใหญ่มีการกระทำเก็บไว้ในแผ่นฟลอปปี้ดิสค์ หรือเทปคาร์ทริดจ์ การสำเนาข้อมูลจำนวนมากจึงต้องเสียเวลาและมีขั้นตอนในการดำเนินการ พึงระลึกเสมอว่า การสำเนาข้อมูลจะไม่กระทำลงบนตัวกลางเดิมที่มีข้อมูลอยู่แล้ว จนกว่าจะมีข้อมูลอีกชุดได้เก็บสำเนาไว้แล้วในที่ ๆ ปลอดภัย

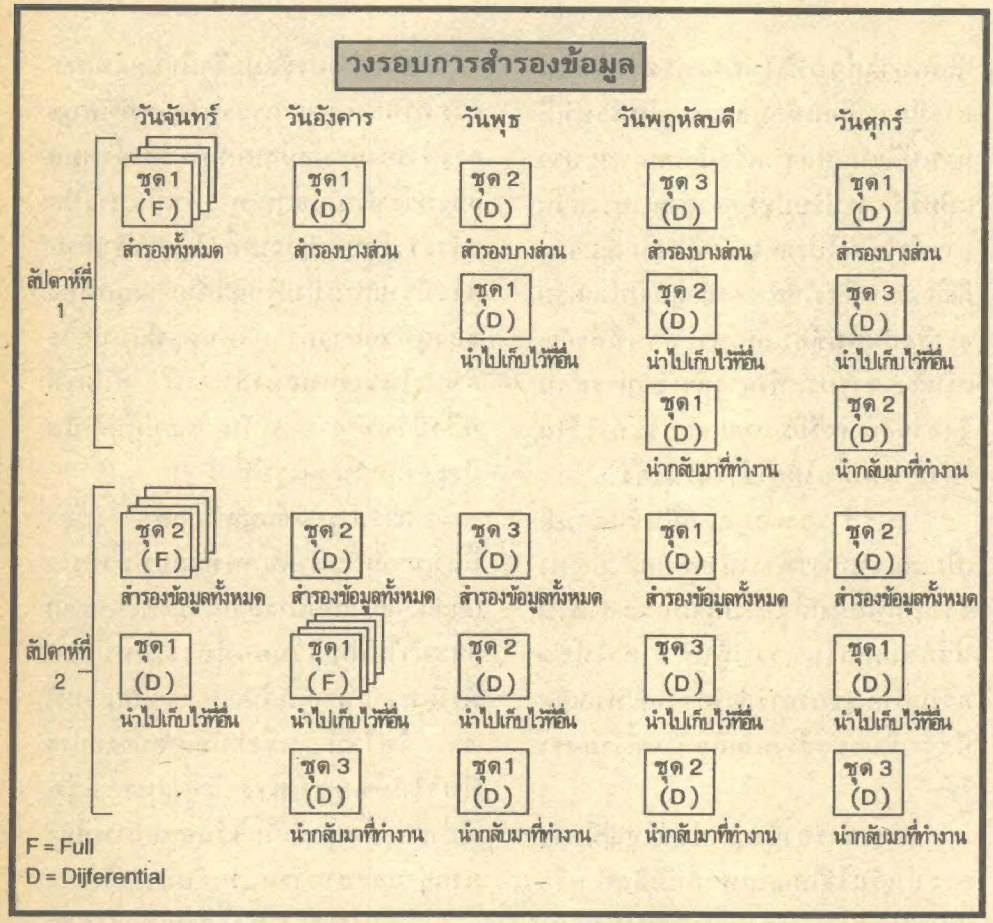
การสำรองข้อมูลจึงมีขั้นตอนและกระทำหลายชุด กระทำโดยสม่ำเสมอ การสำรองข้อมูลมีแบบที่กระทำทั้งหมดและกระทำบางส่วน การดำเนินการมักสร้างวงรอบที่ชัดเจนเพื่อให้การดำเนินการมีรูปแบบที่ปฏิบัติได้อย่างถูกต้อง ลองดูตัวอย่างการกำหนดรูปแบบการสำเนาในวงรอบสองสัปดาห์ สัปดาห์หนึ่งมีวันทำงาน 5 วัน โดยปฏิบัติเป็นประจำทุกวัน ดังรูปที่ 1

การสำรองข้อมูลที่ถูกต้องจึงต้องมีสำเนาที่เป็นลำดับกันทั่วแบบทั้งหมด (Full) และแบบบางส่วน (Differential) และนำไปเก็บไว้นอกที่ทำงานหนึ่งชุด ทั้งนี้เพราะหากเกิดปัญหาเรื่องสถานที่ เช่น ไฟไหม้ หรืออุบัติเหตุบางอย่างที่ทำให้ข้อมูลที่ทำงานสูญหายหรือเสียหาย ข้อมูลที่เก็บไว้นอกสถานที่ยังคงอยู่ และสามารถนำกลับมาใช้ได้

จะเห็นได้ว่าวงรอบการสำรองข้อมูลขณะใดขณะหนึ่งจะมีสำเนาที่เป็นฉบับเต็มเก็บไว้ที่ทำงานหนึ่งชุด และนอกที่ทำงานหนึ่งชุด ส่วนฉบับสำรองบางส่วนมีเก็บไว้ที่ทำงานสองชุด และที่ภายนอกหนึ่งชุด การนำกลับมาสำเนาใหม่จะเวียนกันสลับไปเรื่อย การสร้างสำเนาที่มีขั้นตอนปฏิบัติเช่นนี้จะสร้างความมั่นใจในการปฏิบัติและเชื่อถือได้ว่าข้อมูลของตนยังคงเก็บไว้ได้เสมอ

การใช้โปรแกรมสำเนาข้อมูล

ในยูทิลิตี้ที่ใช้มีหลายโปรแกรมให้ใช้ ในระบบดอสที่เป็นที่รู้จักกันดีมีโปรแกรมให้เลือกใช้ เช่น โปรแกรม Backup, Restore โปรแกรม Copy โปรแกรม Xcopy หรือโปรแกรม Backup เฉพาะที่มีมาให้ ในที่นี้จะขอกล่าวถึงโดยสรุป



รูปที่ 1 แสดงวงรอบการแสดงข้อมูล

- โปรแกรม DOS Backup เป็นโปรแกรมที่ไม่ค่อยแนะนำให้ใช้ เพราะโปรแกรม Backup จะทำการคัดลอกทั้งหมดลงในฟลอปปี้ดิสก์ ซึ่งอาจต้องใช้ดิสเกตต์หลาย ๆ แผ่นต่อเนื่องกัน และหากการใช้งานมีแผ่นดิสเกตต์แผ่นใดแผ่นหนึ่งมีปัญหา ก็จะทำให้ข้อมูลที่สำเนาทั้งหมดมีปัญหาไม่สามารถทำการ Restore หรือนำกลับมาใช้ใหม่ได้

- โปรแกรม Xcopy เป็นโปรแกรมที่เหมาะสมกับการนำมาใช้งานมาก เพราะสามารถเลือก Copy เป็นไดเรคทอรีรวมไดเรคทอรีย่อย หรือใช้ในการ Copy เป็นบางส่วนโดยเลือกตามวันที่ หรือจะกำหนดการเลือกตามแอตทริบิวต์ของไฟล์ได้ โปรแกรม Xcopy จึงนำมาใช้ประโยชน์ในการสำเนาข้อมูลที่ดีได้

- โปรแกรมยูทิลิตี้การสำรองข้อมูล ปัจจุบันมีโปรแกรมสำรองข้อมูลที่ให้เพิ่มเติมเข้ามาหลายโปรแกรม เช่น ในดอส 6.0 มีโปรแกรม NortonBackup และในพีซีดอส 6.1 ก็มี Central Point Backup โปรแกรมเหล่านี้ได้เพิ่มขีดความสามารถพิเศษในการสำรองข้อมูลไว้มากเช่น การสำรองข้อมูลแบบบีบอัดให้ข้อมูลใช้ที่เก็บน้อยลง มีการตรวจสอบข้อผิดพลาด และยังมีความเชื่อถือในการแบคอัพได้ดีมีความเร็วในการทำงานสูง

- โปรแกรม Backup เฉพาะ มีบริษัทอื่นที่ผลิตโปรแกรม Backup ออกขายหลายบริษัท โปรแกรมเหล่านี้มักเพิ่มเติมขีดความสามารถเฉพาะบางอย่างเข้าไป เช่น ระบบการแก้ไขข้อผิดพลาด ระบบการเลือกสำรองข้อมูล ระบบการตรวจสอบและเชื่อมโยงใช้งานกันบนเครือข่าย เป็นต้น

ป้องกันข้อมูลจากการเรียกดูของผู้ไม่เกี่ยวข้อง

ข้อมูลทางธุรกิจเป็นสิ่งที่สำคัญและมีคุณค่า โดยเฉพาะในยุคของการแข่งขัน สิ่งที่จำเป็นคือการป้องกันข้อมูลไม่ให้หลุดไปอยู่ในมือของคู่แข่งขันทางการค้า การป้องกันข้อมูลในระดับนี้เป็นระดับที่หลายธุรกิจให้ความสำคัญ แต่บางธุรกิจก็ให้ความสำคัญน้อยลง การป้องกันนี้นอกจากจะป้องกันในระดับที่เป็นคู่แข่งการค้าแล้ว บางครั้งฝ่ายบริหารป้องกันความลับของข้อมูลไม่ให้รั่วไหลลงไปในระดับปฏิบัติงาน

หากข้อมูลที่เก็บไว้มีคุณค่าและมีความสำคัญ การโจรกรรมหรือการแอบค้นข้อมูลก็จะมีมากขึ้น และที่สำคัญคือบางแห่งอาจจะมีการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การกระทำในลักษณะนี้สร้างความเสียหายให้กับองค์กรได้

ปัญหาส่วนใหญ่อยู่ที่บุคคล

ข้อมูลข่าวสารที่เก็บไว้ในคอมพิวเตอร์และมีผู้ใช้ร่วมกันได้หลายคน ดังนั้นการรั่วไหลของข้อมูลจึงขึ้นอยู่กับบุคคล บุคคลที่ใช้คอมพิวเตอร์ใช้เวลาเพียงเล็กน้อยก็สามารถคัดลอกข้อมูลลงในแผ่นดิสเกตต์ หรือสั่งโอนย้ายข้อมูลไปเก็บไว้ที่อื่นได้อย่างรวดเร็วจำนวนมาก ยิ่งในปัจจุบันการเชื่อมโยงเครือข่ายเป็นไปอย่างกว้างขวาง การแอบคัดลอกข้อมูลแล้วส่งถ่ายไปยังที่ห่างไกลทำได้อย่างง่ายดาย ปัญหาของ

การป้องกันการรั่วไหลหรือการเข้ามาเปลี่ยนแปลงข้อมูลจึงอยู่ที่บุคคล เรามีวิธีการป้องกันบุคคลที่ไม่มีสิทธิในการเข้าถึงข้อมูลได้หลายวิธี มีการนำมาประยุกต์ใช้ในระดับต่าง ๆ กันอยู่มาก เช่น ใช้โปรแกรมควบคุมอยู่ในโปรแกรมประยุกต์ ใช้รหัสผ่าน (password) ใช้วิธีการเอ็นคริปชั่นข้อมูล วิธีการเหล่านี้เป็นเพียงส่วนหนึ่งของการป้องกัน

การใช้ซอฟต์แวร์ควบคุม

ซอฟต์แวร์ประยุกต์หลายโปรแกรมมีการผนวกระบบรักษาความปลอดภัยไว้ในตัวด้วย เช่น ซอฟต์แวร์จัดการฐานข้อมูล มีการกำหนดผู้เข้าถึงที่จะเรียกเข้าหาไฟล์หรือเปิดฐานข้อมูล มีการให้สิทธิในระดับต่าง ๆ ซึ่งผู้พัฒนาโปรแกรมสามารถกำหนดสิทธิของผู้ใช้ในระดับต่าง ๆ เพื่อว่าผู้ใช้จะเข้าถึงข้อมูลในขอบเขตที่วางไว้เท่านั้น

การควบคุมในลักษณะนี้มีในโปรแกรมจัดระบบงานอยู่แล้ว เช่น ในโปรแกรมจัดการเครือข่ายเน็ตแวร์ก็มีการกำหนดการรักษาความปลอดภัย มีการให้ใช้รหัสผ่านเมื่อต้องการล็อกเข้ามาเป็นผู้ใช้ เพื่อให้โปรแกรมตรวจสอบ หากใช้รหัสผ่านผิดสามครั้งก็จะไม่ให้เรียกเข้ามาใช้อีก

รหัสผ่านเป็นเรื่องสำคัญ

วิธีกำหนดผู้เข้าใช้ในระบบที่นิยมใช้มากในขณะนี้คือการใช้รหัสผ่าน เครื่องคอมพิวเตอร์รุ่นใหม่มีการกำหนดรหัสผ่านเพื่อเรียกการใช้เริ่มต้น ดังนั้นผู้เปิดเครื่องครั้งแรกจะต้องป้อนรหัสผ่าน ถ้ารหัสผ่านถูกต้องจึงจะดำเนินการต่อไปได้ ในระบบเน็ตแวร์ก็มีการใช้รหัสผ่าน ระบบยูนิกซ์ก็มีการใช้รหัสผ่าน รหัสผ่านจึงเป็นเรื่องสำคัญที่ใช้ในการป้องกันผู้ไม่มีสิทธิในการใช้งาน อย่างไรก็ดี หากรหัสผ่านไม่ดีพอ ผู้ลักลอบสามารถคาดเดาได้ การเรียกเข้าใช้ในระบบก็เป็นไปได้ ปัจจุบันบนเครือข่ายอินเตอร์เน็ตมีการสร้างโปรแกรม worm ที่ทำการเจาะค้นหารหัสผ่านของระบบที่ง่ายต่อการถอดรหัส และเข้าไปในระบบเพื่อดำเนินการอย่างอื่นต่อไปได้

ลักษณะของรหัสผ่านที่ดีควรมีลักษณะอย่างไร สิ่งนี้มีการพูดคุยกันมาก แต่จากการได้มีโอกาสสัมผัสกับโปรแกรม crack ซึ่งเป็นโปรแกรมที่ผู้พัฒนาขึ้นมาเพื่อใช้ในการถอดรหัสผ่านของผู้ใช้ในระบบยูนิกซ์ และผู้เขียนมีโอกาสนำมาทดลองใช้กับผู้ใช้งานบนเครื่องที่มีประมาณ 800 คน ใช้เวลาในการ crack ประมาณ 1 ชั่วโมง สามารถได้รหัสผ่านของผู้ใช้ในระบบประมาณ 20 คน นั่นหมายความว่ามีผู้ใช้จำนวนไม่น้อยที่ตั้งรหัสผ่านที่ง่ายต่อการถอดรหัส

รหัสผ่านที่ดีควรมีลักษณะดังต่อไปนี้

- ไม่ควรใช้ชื่อเฉพาะ หรือชื่อตัวใด ๆ มาใช้ แม้จะเป็นส่วนหนึ่งของชื่อ
- ไม่ควรใช้คำที่ปรากฏในพจนานุกรม
- ไม่ควรใช้ข้อมูลส่วนบุคคลมาเป็นรหัสผ่าน เช่น รหัสบัตรประจำตัว รหัสใบขับขี่ หรือวันเดือนปีเกิด
- ไม่ควรใช้ชื่อ userid หรือแม้แต่การสลับไปมาจากชื่อนั้น
- ไม่ควรใช้ตัวอักษรหรือตัวเลขที่เหมือนกันซ้ำ ๆ กันหลายตัว
- ให้รหัสผ่านมีอักขระพิเศษเช่นตัวเลขปนอยู่ด้วย
- ให้ใช้รหัสผ่านที่มีความยาวไม่น้อยกว่า 7 ตัวอักษร
- ใช้รหัสผ่านที่คุณสามารถพิมพ์ลงไปได้อย่างรวดเร็ว เพื่อหลีกเลี่ยงการสังเกตของผู้อยู่ใกล้เคียง
- ให้รหัสผ่านเป็นรหัสที่จำได้ไม่ผิดพลาด
- ไม่ควรเขียนรหัสผ่านไว้ที่ใดหรือนำรหัสผ่านไปใช้ร่วมกับผู้อื่น และให้เปลี่ยนรหัสผ่านบ่อย ๆ และอย่าใช้รหัสผ่านเก่าที่เคยเลิกใช้ไปแล้ว

ป้องกันข้อมูลโดยการเอ็นคริปชั่น

- หากมีผู้เข้าถึงข้อมูลได้และคัดข้อมูลไป หนทางที่จะป้องกันคือ ให้มีการเอ็นคริปข้อมูลเพื่อว่าข้อมูลนั้นจะยากต่อการถอดรหัสออกมาดูได้ ปัจจุบันมีโปรแกรมที่ใช้ในการดำเนินการเช่นนี้หลายโปรแกรม เช่น ยูทิลิตี้ในการบีบอัดข้อมูลก็เป็นวิธีการเอ็นคริปวิธีการหนึ่ง เช่น โปรแกรม stacker ทำการบีบอัดข้อมูล PKZIP ก็เป็นอีกโปรแกรมหนึ่ง การบีบอัดแบบเอ็นคริปชั่นนี้มีการกำหนดคีย์หรือเสมือนเป็นรหัสที่จะใช้ในการถอดรหัสกลับ ดังนั้นถ้าหากลืมรหัสคีย์ ข้อมูลนั้นจะไม่สามารถเรียกดูได้อีกต่อไป การเอ็นคริปจึงต้องระมัดระวังในเรื่องคีย์เป็นพิเศษ

ระวังคนข้างหลัง

คนข้างหลังในความหมายนี้คือบุคคลที่ร่วมงานกับเรา บุคคลที่สามารถเข้าถึงระบบได้ ซึ่งอาจจะผ่านเข้าทางเครือข่าย หรือระบบที่สามารถเรียกเข้าหาได้จากระยะไกล เช่น เรียกจากโมเดม การดำเนินการในลักษณะนี้จึงต้องให้ความสำคัญว่าคนใกล้ชิดก็มีโอกาสทำให้ข้อมูลรั่วไหลได้ ข้อมูลเหล่านี้สามารถเรียกค้นดูในระยะไกลโดยที่เจ้าตัวไม่รู้ เช่น ในเครือข่าย

อินเตอร์เน็ตสามารถใช้คำสั่ง FTP เข้ามาในระบบแล้วสั่งโยกย้ายแฟ้มไปได้ โดยที่หากระบบป้องกันไม่ดี ข้อมูลก็จะได้รับการโอนย้ายไปได้โดยง่าย

ไวรัสปัญหาที่เกิดขึ้นได้เสมอ

ไวรัสเป็นปัญหาที่ทำให้เกิดการสูญหายกับข้อมูลและโปรแกรมได้เป็นอย่างมาก มีไวรัสที่แพร่หลายอยู่ทั่วไปเป็นพันตัว และมีไวรัสเกิดขึ้นใหม่อย่างต่อเนื่อง แพร่หลายกระจายไปได้อย่างรวดเร็ว จากปัญหาของไวรัสทำให้การใช้งานคอมพิวเตอร์เป็นปัญหาเกิดขึ้นได้เสมอ และผู้ใช้คอมพิวเตอร์จะเสี่ยงต่อการติดไวรัสได้

ไวรัสเป็นโปรแกรมคอมพิวเตอร์ที่แทรกตัวเองปะปนไปกับแผ่นดิสเกตต์และคัดลอกไปยังที่ต่าง ๆ ได้ถ้ามีโอกาส หากพบเงื่อนไขเหมาะสมก็จะทำลายข้อมูลหรือโปรแกรมสร้างปัญหาให้กับผู้ใช้ตลอดมา

ข้อแนะนำในทางปฏิบัติเกี่ยวกับปัญหาไวรัส

เพื่อหลีกเลี่ยงปัญหาไวรัสที่อาจเกิดขึ้นได้กับคุณและองค์กรของคุณ จึงมีข้อแนะนำในทางปฏิบัติ เพื่อหลีกเลี่ยงปัญหาที่อาจจะเกิดกับข้อมูลอันเนื่องมาจากไวรัส ข้อแนะนำเล็ก ๆ น้อย ๆ เหล่านี้เป็นสิ่งที่ควรปฏิบัติ

- ให้ติดตั้งโปรแกรมสแกนตรวจสอบไวรัสไว้ภายในเครื่อง เพื่อคอยเฝ้าติดตามตั้งแต่การบูตเครื่อง การคัดลอกแฟ้ม หรือตรวจสอบการเปลี่ยนแปลงอันเป็นผลมาจากไวรัส

- ในองค์กรหรือในหน่วยงานควรมีผู้รับผิดชอบในการปรับปรุงโปรแกรมสแกนไวรัส และตรวจสอบการทำงานของโปรแกรมเหล่านี้

- ให้ดำเนินการหาโปรแกรมดอสที่บูตได้โดยปราศจากไวรัสอย่างแน่นอน ทำการติดป้องกันการเขียนและประจำไว้กับเครื่องทุกเครื่อง

- ให้สแกนแผ่นดิสเกตต์ทุกแผ่นที่นำมาจากภายนอก ตรวจสอบให้แน่ใจว่าไม่มีไวรัส จึงยินยอมให้นำมาใช้ได้

- หากมีการดาวน์โหลดไฟล์จากที่อื่นให้ตรวจสอบไวรัสก่อน

- เมื่อมีการนำเครื่องไปซ่อมหรือโอนย้ายเครื่องให้ตรวจสอบไวรัสก่อนการใช้งานใด ๆ

- ไม่ควรต่อพีซีเข้ากับเครือข่ายหากไม่มีระบบสแกนป้องกันไวรัส

- การเชื่อมโยงหรือการ log เข้าไปยังเครือข่าย พึงระลึกว่ามีโอกาสที่จะนำไวรัสมาได้มาก พึงตรวจสอบเป็นประจำก่อนและหลังการใช้งาน

หากพบปัญหาไวรัส

หากพบปัญหาไวรัส หรือสแกนพบไวรัส สิ่งที่ต้องกระทำมีดังต่อไปนี้

- อย่าตกใจ

- อย่ารันโปรแกรมใด ๆ

- ให้บันทึกลักษณะที่พบไวรัสขณะนั้น

- ปิดเครื่อง และเรียกหาผู้เชี่ยวชาญให้มาดูให้ ถ้าหาได้

- ให้ใส่แผ่นบูตที่ปราศจากไวรัสที่มีการป้องกันการเขียนแล้วบูตระบบ

- รันยูทิลิตี้ที่ใช้ในการตรวจสอบไวรัส แผ่นดิสค์ที่ใช้รันต้องติดป้องกันการเขียน

- ทำการฆ่าไวรัสตามขบวนการที่โปรแกรมยูทิลิตี้กำหนดไว้ ให้ทำตามขั้นตอนที่กำหนด

- ให้สแกนดิสเกตต์แผ่นอื่นด้วยเพื่อความมั่นใจ

- ให้ตรวจสอบระบบเครือข่ายดูว่าหนทางการกระจายหรือเครื่องพีซีอื่นในระบบมีปัญหาไวรัสหรือไม่ หากมีต้องดำเนินการให้หมด มิฉะนั้นไวรัสจะเข้ามาอีก โดยพยายามดูแหล่งต้นเหตุและกำจัดให้หมด

- บูตเครื่องใหม่และใช้งานตามปกติ

ป้องกันการถูกขโมยไปทั้งเครื่อง

เนื่องจากพีซีมีขนาดเล็ก หากสิ่งที่คุณเก็บไว้มีค่าสูง มีความเป็นไปได้ที่จะมีความพยายามที่จะขโมยพีซีคุณไปทั้งเครื่อง หนทางป้องกันในกรณีนี้จึงเป็นเรื่องที่คุณจะต้องหาทางป้องกันเอง เช่น เก็บพีซีไว้ในที่ปลอดภัย มีประตูหน้าต่างแน่นหนา มีการล็อกพีซีไว้กับโต๊ะ หรือยึดติดกับสถานที่ วิธีการเหล่านี้เป็นหนทางที่แต่ละท่านจะคิดหาหนทางกันเอาเอง

อนาคตอยู่ที่จริยธรรม

การที่คอมพิวเตอร์จำนวนมากเชื่อมโยงเข้าเป็นเครือข่าย โอกาสของการละเมิดสิทธิเพื่อเข้าถึงข้อมูลที่ไม่มีสิทธิ์จึงมีมากขึ้น หนทางในอนาคตจึงเป็นเรื่องที่จะมีปัญหามากยิ่งขึ้น เพราะเทคโนโลยีที่พัฒนาขึ้นมาก การดำเนินการต่าง ๆ ก็มีการพัฒนาตามไป หนทางที่จะลดปัญหาเหล่านี้ลงจึงอยู่ที่การสร้างจิตสำนึกทางด้านจริยธรรมของผู้ใช้ ไม่ให้ละเมิดสิทธิของผู้อื่น หรือแสวงหาประโยชน์ในทางที่ผิด